AO 106 (Rev. 04/10) Application for a Search Warrant

# United States District Court

for the
Western District of New York

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address.)*

**461 North Star Road, East Aurora, NY 14052**

**Case No. 17-M-** 1125

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

461 North Star Road, East Aurora, NY 14052, as further depicted in Attachment A

located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, the Items to be Searched and Seized

The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and (b)(1), and 2252A(a)(5)(B) and (b)(2).

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

KATHRYN M. GAMBLE
SPECIAL AGENT
HOMELAND SECURITY INVESTIGATIONS
*Printed name and title*

Sworn to before me and signed in my presence.

Date: August 31, 2017

*Judge's signature*

JEREMIAH J. McCARTHY
UNITED STATES MAGISTRATE JUDGE
*Printed name and Title*

City and state: Buffalo, New York

# AFFIDAVIT

STATE OF NEW YORK )
COUNTY OF ERIE ) SS:
CITY OF BUFFALO )

I, Kathryn M. Gamble, being duly sworn, depose and state the following:

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI). I have been employed as a Special Agent since June 2008. I am currently assigned to the HSI Special Agent in Charge in Buffalo, New York. As part of my daily duties as a Special Agent with HSI, I investigate crimes involving child exploitation and child pornography including violations pertaining to the transportation, production, distribution, receipt, and possession of child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. I have received formal and on the job training in the area of child pornography and child exploitation. I have participated in the execution of numerous search warrants involving child pornography and the seizure of computers and other storage media, and I have interviewed many individuals involved in child pornography and the sexual exploitation of children. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

2. This affidavit is submitted in support of an application for a search warrant for the locations specifically described in Attachment A of this Affidavit, **461 North Star Road, East Aurora, NY 14052** (the "SUBJECT PREMISES"), which is more particularly described in Attachment A, and the seizure of the items more particularly described in Attachment B.

As set forth in more detail below, I am investigating the activities of a person who used a computer connecting to the internet to knowingly violate Title 18, United States Code, Section 2252A(a)(2)(A) (receipt and distribution of child pornography) and Title 18, United States Code, Section 2252A(a)(5)(B) (possession of child pornography). As will be shown, there is probable cause to believe that fruits, evidence, and instrumentalities relating to these violations are located at SUBJECT PREMISES.

3. All information contained in this affidavit is either personally known by me or has been related to me by other law enforcement agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt, Transportation, and Distribution of Child Pornography, and Title 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2), Possession of Child Pornography, are presently located at the SUBJECT PREMISES.

## STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1) prohibits a person from knowingly receiving, distributing, or conspiring to receive or distribute, or attempting to do so, any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of

interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and

b. 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

## DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment B:

a. "Child Pornography" is any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

c. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. *See* 18 U.S.C. § 2256(2).

e. "Computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1).

f. "Computer hardware" consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices), peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software" is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer

software is stored in electronic, magnetic or other digital form. It commonly includes computer operating systems, applications and utilities.

h. "Computer-related documentation" consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software or other related items.

i. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to unlock particular data security devices. Data security hardware may include encryption devices, chips and circuit boards. Data security software of digital code may include programming code that creates test keys or hot keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide or booby-trap protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

j. "Internet Service Providers or ISPs" are commercial organizations, which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or coaxial cable data transmission, dedicated circuits or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth,

which the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a coaxial cable system, and can access the Internet by using his or her account name and password.

k. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files.

l. "Internet Protocol address or IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a subscriber's computer at varying intervals at the discretion of the ISP. IP addresses might also be static meaning an ISP assigns a user's computer a specific IP address which is used each time the computer accesses the Internet.

m. "The terms records, documents and materials" include all information recorded in any form, visual or aural, and by any means, whether in hand-made form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, printing and/or typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

n. "Digital device" includes any electronic system or device capable of storing, processing, interpreting or rendering data in digital form, including computer systems of various form factors (computer desktop systems, towers, servers, laptops, notebooks and netbooks), personal digital assistants, cellular telephones and smart phones, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors and drives intended for removable media; related communication devices such as wired and wireless home routers and modems; storage media such as electro-mechanical hard disks, solid state hard disks, hybrid hard disks, floppy disks, optical disks such as compact disks and digital video disks, magnetic tapes and volatile and non-volatile solid state flash memory chips; and security devices including dongles and flash chips.

o. "Image or copy" refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. Imaging or copying maintains contents, but attributes may change during the reproduction.

p. "Hash value" refers to a value generated after data has been subjected to a cryptographic mathematical algorithm. A hash value is akin to a digital fingerprint in that dissimilar data will not produce the same hash value after being subjected to the same hash algorithm. Therefore, a hash value is particular to the data from which the hash value was generated. Known hash values can be used to search for identical data stored on various digital devices and/or media as identical data will have the same hash value.

q. "Compressed file" refers to a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.

## BACKGROUND ON COMPUTERS, CHILD PORNOGRAPHY AND ONLINE CHILD EXPLOITATION

6. I have been formally trained in the investigation of crimes involving the sexual exploitation of children. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet since approximately 1997. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

7. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. Computer technology and the Internet revolutionized the way in which child pornography is produced, distributed, stored and communicated as a commodity and a further tool of child exploitation. For instance:

a. Individuals can transfer photographs from a camera onto a computer-readable format with a variety of devices, including scanners, memory card readers, or directly from digital cameras, including those on most cellphones.

b. Modems allow computers to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

c. The capability of a computer to store images in digital form makes the computer itself an ideal repository for child pornography. As explained further below, personal ownership and quantity of electronic media in use worldwide, and the storage capacity of home computers and other media, have increased tremendously in the last decade and continue to grow. Computer drives and other electronic storage media can store a huge amount of visual images at very high resolution.

d. The Internet, the World Wide Web and other Internet components afford individuals many different and relatively secure and anonymous venues for obtaining, viewing and trading child pornography or for communicating with others to do so or to entice children.

e. Individuals can use online resources to retrieve, store and share child pornography, including services offered by Internet Portals such as Google, America

Online (AOL), Yahoo! and Hotmail, among others. Online services allow a user to set up an account providing e-mail and instant messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer or cellular phone with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, evidence of child pornography can be found on the user's computer in most instances.

f. As is the case with most digital technology, computer communications can be saved or stored on hardware and computer storage media used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite web sites in, for example, bookmarked files. However, digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or footprints in the web cache and history files of the browser used. Such information is often maintained for very long periods of time until overwritten by other data.

g. The interaction between software applications and the computer operating systems often results in material obtained from the Internet being stored multiple times, and even in different locations, on a computer hard drive without the user's knowledge. Even if the computer user is sophisticated and understands this automatic storage of information on his computer's hard drive, attempts at deleting

the material often fail because the material may be automatically stored multiple times and in multiple locations within the computer media. As a result, digital data that may have evidentiary value to this investigation could exist in the user's computer media despite, and long after, attempts at deleting it. A thorough search of this media could uncover evidence of receipt, distribution and possession of child pornography.

h. Data that exists on a computer is particularly resilient to deletion. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person deletes a file on a home computer, the data contained in the file does not actually disappear, rather, the data remains on the hard drive until it is overwritten by new data. Therefore, deleted files or remnants of deleted files, may reside in free space or slack space, that is, in space on the hard drive that is not allocated to an active file and is left unused and free to store new data. Such residual data may remain in free space for long periods of time before it is overwritten by new data. In addition, a computer's operating system may also keep a record of deleted data in a swap or recovery file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic

file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity and computer habits.

## KIK MESSENGER APPLICATION

8. The Kik Messenger application is primarily a social media mobile device platform designed and managed by Kik Interactive Incorporated, a Waterloo, Canada based company, for the purpose of mobile messaging and communication. To use this application, a user downloads the mobile messaging application via an applications service such as the Google Play Store, Apple Itunes, or other similar mobile application provider. Once downloaded and installed, the user is prompted to create an account and a username. This username will be the primary account identifier. The user also has a display name, which will be what other users initially see when transmitting messages back and forth. As part of the account creation process, Kik users are asked to supply a valid email address, create a password, provide an optional date of birth, and user location. The user also has the option of uploading a "profile avatar" that is seen by other users Once the Kik user has created an account, the user is able to locate other users via a search feature. The search feature usually requires the user to know the intended recipient's username. Once another user is located or identified, Kik users can send messages, images, and videos between the two parties.

9. Kik Messenger also allows users to create chat rooms, of up to 50 people, for the purpose of communicating and exchanging images and videos. These rooms are administered by the creator who has the authority to ban and remove other users from the created room. According to Kik Messenger, more than 40% of the Kik users chat in "groups" and approximately 300,000 new groups are created every day. These groups are frequently

created with a "hashtag" allowing the group or chat to be identified more easily. Once the group or chat is created Kik users have the option of sharing the "link" with all of their contacts or anyone they wish.

## BACKGROUND ON COMPUTERS AND EVIDENCE ASSESSMENT PROCESS IN CHILD PORNOGRAPHY AND CHILD EXPLOITATION INVESTIGATION

10. This warrant seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for evidence that establishes how computing devices were used, the purpose of their use, and who used them.

11. As described above, and in Attachment B, this application seeks permission to search and seize certain digital evidence that might be found in the SUBJECT PREMISES, in whatever form it is found. One form in which the records might be found is stored on a computer's hard drive, mobile computing device, or other electronic media. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. In addition to user-generated documents (such as messages, picture and movie files), computing devices can contain other forms of electronic evidence that are not user-generated. In particular, a computing device may contain records of how a computer or mobile device has been used, the purposes for which it was used and who has used these records, as described further in the attachments.

12. Based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I

know that segregating information before commencement of the review of digital evidence by the examining agent is inconsistent with the evidence assessment process in child pornography and online child exploitation investigations. This is true in part because the items to be searched will not only contain child pornography, but also will contain the identity of the user/possessor of the child pornography as well as evidence as to the programs and software used to obtain the child pornography, which may be located throughout the areas to be searched. In addition, it is not possible to know in advance which computing device or storage media will contain evidence of the specified crimes, and often, such evidence is contained on more than one computer/device or digital storage device. Further:

a. Searching digital devices can be a highly technical process that requires specific expertise, specialized equipment and knowledge of how electronic and digital devices are often used in child pornography and online child exploitation matters. There are so many types of digital devices and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search.

b. Because of the numerous types of digital devices and software that may contain evidence in child pornography and online child exploitation cases, it may also be necessary to consult with specially trained personnel who have specific expertise in the type of digital device, software application or operating system that is being searched in an off-site and controlled laboratory environment.

c. Because digital data is particularly vulnerable to inadvertent or intentional modification or destruction, searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital

data and to recover "hidden," erased, compressed, encrypted or password-protected data. Data hiding analysis can be useful in detecting and recovering such data and may indicate knowledge, ownership, or intent. The recovery of "hidden" data is highly specialized and time-intensive. For this reason, on-site key word searches are not sufficient to recover inadvertently or intentionally modified or destroyed data. Similarly, running hash values on-site to find files that contain child pornography is not an adequate on-site review and seizure procedure, because while hash values locate previously identified files of child pornography, they do not capture files that are the result of new production, images imbedded in an alternative file format, or images altered, for instance, by a single pixel. As a result, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of data stored on digital devices.

d. The volume of data stored on many digital devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 240 million pages of data. Further, a 500 GB drive could contain as many as approximately 450 full run movies or 450,000 songs. As examining this quantity of data can take weeks or months, depending on

the volume of the data stored, it would be impractical to attempt this kind of data search on-site.

e. Electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files saved to a hard drive can be stored for years with little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Recovery of residue of electronic files from a hard drive requires specialized tools and a controlled laboratory environment.

f. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Digital device users may also attempt to conceal data by using encryption, which means that a password or physical device,

such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. "Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed." A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband or instrumentalities of a crime.

g. Further, in finding evidence of how a computer has been used, the purposes for which it was used, and who has used it, sometimes it is necessary to establish that a particular thing is not present on a hard drive or that a particular person (in the case of a multi-user computer) was not a user of the computer during the time(s) of the criminal activity. For instance, based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of digital devices, I know that when a computer has more than one user, files can contain information indicating the dates and times that files were created as well as the sequence in which they were created, so that evidence of whether a user accessed other information close in time to the file creation dates, times and sequences can help establish user identity and exclude other users from computer usage during relevant times.

h. Because the absence of particular data on a digital device may provide evidence of how a digital device has been used, what it has been used for, and who has

used it, analysis of the digital device as a whole may be required to demonstrate the absence of particular data. Such evidence of the absence of particular data on a digital device is not segregable from the digital device.

i. The types of evidence described above may be direct evidence of a crime, indirect evidence of a crime indicating the location of evidence or a space where evidence was once located, contextual evidence identifying a computer user, and contextual evidence excluding a computer user. All of these types of evidence may indicate ownership, knowledge, and intent. This type of evidence is not "data" that can be segregated, that is, this type of data cannot be abstractly reviewed and filtered by a seizing or imaging agent and then transmitted to investigators. Rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves and how computers are used. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

j. Based upon my knowledge, training and experience, as well as information relayed to me by agents and others involved in the forensic examination of digital devices, I know that it is typically necessary to seize all types of electronic devices capable of storing digital evidence as described in the Affidavit and Attachment B for off-site review because computer searches involve highly technical, complex, time-consuming and dynamic processes.

## SEARCH METHODOLOGY TO BE EMPLOYED

13. As noted within this search warrant, it would be extremely difficult, if not impossible to conduct a thorough on-site review of all of the potential evidence in this case.

Given these constraints, the search methodology to be employed as to computers and digital media is as follows:

a. All computing devices, computer hardware and any form of electronic storage that could contain evidence described in this warrant will be seized for an off-site search for evidence that is described in the attachments of this warrant. It is anticipated that mirror copies or images of such evidence will be made if the failure to do so could otherwise potentially alter the original evidence.

b. Consistent with the information provided within this affidavit, contextual information necessary to understand the evidence, to identify the user/possessor of the child pornography, and to establish admissibility of the evidence in subsequent legal proceedings will also be sought by investigative agents.

c. Additional techniques to be employed in analyzing the seized items will include (1) surveying various file directories and the individual files they contain; (2) opening files to determine their contents; (3) scanning storage areas; (4) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in this affidavit and its attachments; and (5) performing any other data analysis techniques that may be necessary to locate and retrieve the evidence described in this affidavit and its attachments.

d. Because it is expected that the computers, mobile computing devices, computer hardware and any form of electronic storage media may constitute (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, or (4) evidence otherwise unlawfully possessed, it is anticipated that such evidence will not

be returned to the owner and that it will be either forfeited or ultimately destroyed in accordance with the law at the conclusion of the case. However, if after careful inspection investigators determine that such computers, computer hardware and electronic storage media do not contain (1) instrumentality of the offense, (2) fruit of criminal activity, (3) contraband, (4) evidence otherwise unlawfully possessed, or (5) evidence of the person who committed the offense and under what circumstances the offense was committed, then such items seized will be returned.

## THE INVESTIGATION AND BACKGROUND

14. On August 22, 2017, while conducting undercover child exploitation investigations on the mobile messaging application KIK messenger ("KIK"), your affiant observed KIK user "ronin777788" enter into public KIK chat group, "Tabu Moms (MOMS ONLY)". After observing "ronin777788" ask another user within the group if they were a mother, and thereafter observing that "ronin777788" subsequently asked to private message with the user when the user replied "yes", your affiant, while using an undercover ("UC") profile, began engaging in private message communication with "ronin777788".

15. During the private message conversation, "ronin777788" asked your affiant, "Do you like younger". After your affiant replied "yes", "ronin777788" sent your affiant a live "selfie" image of himself. The image sent by "ronin777788" depicts a white male, approximately fifty years old, with light brown hair, in an outdoor setting.

16. During the private message conversation, "ronin777788" told your affiant that he resides in East Aurora, New York, that his name is George, that he is forty-four years old, that he has a ten year old son, that he is interested in both boys and girls, and that he is "not really" active with his son. User "ronin777788" also told your affiant that he is a Registered Nurse and works in downtown Buffalo.

17. On August 23, 2017, at approximately 3:10 PM EST, "ronin777788" asked your affiant, while she was using a UC profile, if she was "able to look at some pics" and "ronin777788" proceeded to send your affiant an image depicting two naked, prepubescent female children lying on top of each other with their vaginas exposed to the camera. User "ronin777788" then told your affiant that he would, "Love to see you licking that", and stated "Lick them together; Spread your legs for her; Push her head down".

18. On August 23, 2017, at approximately 4:07 PM EST, "ronin777788" sent your affiant a video file depicting a minor female, approximately thirteen years old, undressing in front of the camera, exposing her vagina to the camera, and then masturbating herself with a hairbrush. Thereafter, "ronin777788" suggested that he and your affiant engage in sexual activity with the female children depicted in the image file that he sent.

19. On August 27, 2017, "ronin777788" sent your affiant another video file. This video depicts a minor female, approximately fifteen years old, naked, masturbating in front of the camera with a hairbrush.

20. On August 23, 2013, a U.S. Immigration and Customs summons was served on KIK relating to user "ronin777788".

21. On August 24, 2017, KIK responded to the summons and provided the following account details:

a. First Name: George

b. Last Name: S

c. Email: gschwab62@icloud.com (unconfirmed)

d. Registration: 2015/09/11 10:08:22

e. Country: US

f. Device type: iphone

g. Wifi IP addresses: 67.241.173.11, 98.4.56.59

22. A query within the MaxMind geolocation online database revealed that both target IP addresses, 67.241.173.11, 98.4.56.59, are located in or near Orchard Park, NY and are registered to the internet service provider (ISP) Time Warner Cable (recently merged with Charter Communications).

23. On August 26, 2017, a U.S. Immigration and Customs Enforcement summons was served on Charter Communications for IP addresses 67.241.173.11 and 98.4.56.59, which were used to access the KIK Messenger application on the dates of some or all of the image/video file and chat postings described above.

24. On August 28, 2017, Charter Communications responded to the summons and identified the account subscriber associated to both IP addresses to be GEORGE SCHWAB at 461 North Star Rd., East Aurora, NY 14052.

25. In addition to the above referenced Wifi IP addresses, the KIK subscriber return showed that user "ronin777788" had numerous connections to an IP address registered to Roswell Park Cancer Institute, in Buffalo, New York.

26. Your affiant compared the live "selfie" image sent by "ronin777788" to the New York State driver's license of GEORGE W. SCHWAB (DOB: 03/23/1962) and discovered that they depict the same individual. Additionally, the background in the image sent by "ronin777788", to your affiant, matches the outdoor setting visible in the backyard at address 461 North Star Rd., East Aurora, NY 14052.

27. Your affiant, using a publically available website, discovered that GEORGE SCHWAB (DOB: 03/23/1962) is listed as a resident of 461 North Star Rd., East Aurora, NY 14052.

## CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

28. Over the course of my law enforcement career, your affiant has conducted and participated in a significant number of investigations concerning online child sexual exploitation, focusing specifically on crimes involving child pornography. Your affiant has personally interviewed child sex offenders who committed online child pornography crimes. Your affiant also has been informed of the studies of child sex offenders in general, and child

pornography offenders in particular. Your affiant also has learned about the activities and characteristics of child pornography offenders from other law enforcement agents who focus on online child sexual exploitation, including those who investigate the offenses and those who analyze the computer equipment of the offenders.

29. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that there are certain characteristics common to many individuals involved in the solicitation, possession, receipt, and distribution of child pornography. Those who solicit, possess, receive, and distribute child pornography:

a. Often receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. May collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner or to demonstrate the desired sexual acts.

c. May possess and maintain hard copies of child pornographic material, such as pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security

of their home or some other secure location. Some of these individuals retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica and videotapes for many years.

d. Often go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They almost always maintain their collections in the privacy and security of their homes, cars, garages, sheds, or other secure storage location, such as on their person. These collections are often maintained for several years and are kept close by, usually at the individual's residence or on the collector's person, to enable the collector to view the collection, which is valued highly.

e. Often possess multiple digital devices, such as desktop and laptop computers, smart phones, tablet computers, etc. and multiple storage devices, such as flash drives and memory, external hard drives, CDs, etc. which are used to access, distribute, and store child pornography. While the storage capacity of such devices can be as large as tens of gigabytes in size and allow for the storage of thousands of images and videos (as well as other digital information such as contact lists, programs and text documents), such storage devices can be smaller than a postage stamp in size, which allows them to be easily concealed, such as in a person's pocket.

f. Tend to keep their older devices even after upgrading to newer technology. The older devices, along with the items stored on them, are often still accessible.

g. May utilize online/remote storage services to store, access, and distribute child pornography. The content stored on online storage services may

accessible through the subject's computer while it is logged in, but may be difficult to obtain once the computer is turned off.

h. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

i. Prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

30. Based on my own experience in investigating computer-facilitated child sexual exploitation crimes, and the experiences of other law enforcement agents with who I have consulted, I believe that the majority of individuals who collect child pornography via the Internet maintain their collections, increasingly in both online and offline storage media, as well as on hard drives of devices and in cloud or other types of virtual or remote storage locations. Doing so allows them to access and maintain their contraband collection even as they move from one physical location to another.

## CONCLUSION

31. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause to believe that evidence, fruits, and instrumentalities of

violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), Receipt, Transportation, and Distribution of Child Pornography and Title 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2), Possession of Child Pornography, are presently located at the SUBJECT PREMISES as described in Attachment A, and will be located on the items more particularly described in Attachment B.

32. In consideration of the foregoing, your affiant respectfully requests that this Court issue a warrant to search the SUBJECT PREMISES as more particularly described in Attachment A, and to seize the items specified in Attachment B.

Kathryn M. Gamble
Special Agent
Homeland Security Investigations

Sworn and subscribed to before me

this 31st day of August, 2017.

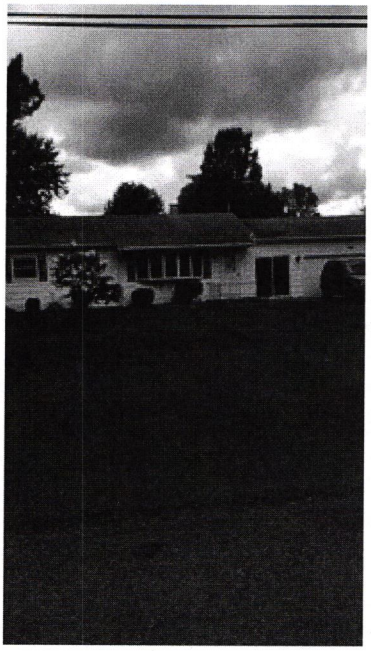
JEREMIAH J. McCARTHY
United States Magistrate Judge

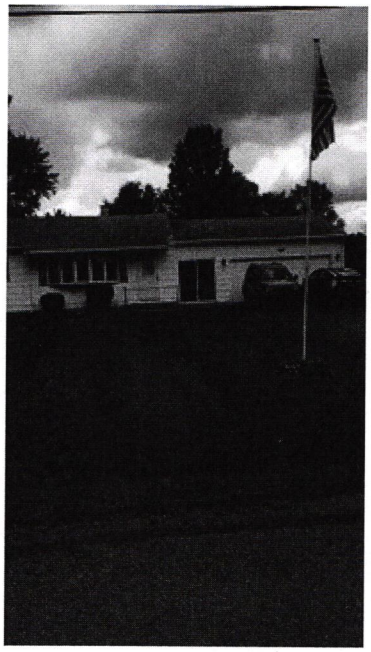
# ATTACHMENT A

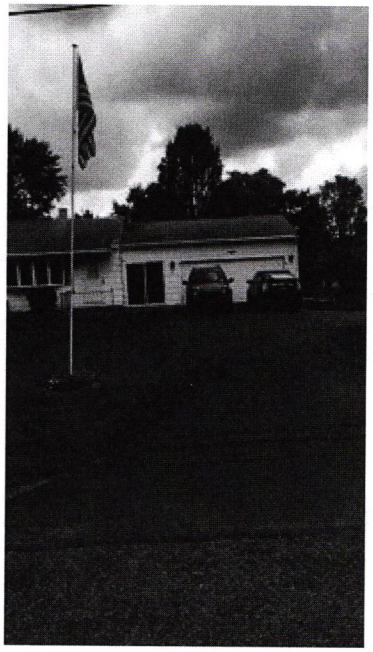
## Description of Premises To Be Searched:

461 North Star Road, East Aurora, NY 14052

Single story, single family residence, white in color with an attached two car garage. The numbers "461" are clearly displayed on the front of the home.







**ATTACHMENT B**
**The Items to be Searched and Seized**

The following items to be seized at the location to be searched listed in **Attachment A**, including items, records, documents, materials and files, whether in physical, documentary, or electronic form, to include:

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any mechanism used for the receipt or storage of the same, including but not limited to:

> Any and all electronic storage device as to which agents reasonably believe that George Schwab has access to including but not limited to any computer, computer system and related peripherals including any data processing devices and software (including but not limited to central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, thumb drives, media cards, zip drives and diskettes, computer compact disks, CD-ROMS, DVDs, SIM cards and any other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, routers, and related communications devices such as cables and connections); related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices and electronic tone-generating devices); cellular telephones; Smart phones; I-phones; PDAs, blackberries, and any electronic devices; and any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks); and any computer or data processing manuals, instruction books or any other documents or records relating to instructions relating to use of computer software or programs.

2. Any access numbers, passwords, personal identification numbers, user names, screen names or internet accounts used, or possibly used, to access any computers, servers, storage devices or Internet web sites for child pornography.

3. Any and all computer passwords, counter-forensic programs, and other data security devices designed to restrict access to, hide, or destroy computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code.

4. Any and all correspondence, documents, records, images, videos, emails, instant messages, or any other type of electronic mail, email software, associated email addresses, email address book contents, chat files, chat logs, chat names used, chatroom contacts, chat software, peer to peer software, peer to peer files, newsgroup postings by the user, IP addresses assigned, and buddy lists, favorites, internet history, browsing history,

internet search history, cookies, deleted files, search terms, screen names, bookmarked and favorite web pages, user typed web addresses, websites visited via desktop shortcuts, path and file names for files opened through any media and/or image viewing software, IP addresses assigned, and other records, correspondence or evidence, pertaining to the receipt, distribution, transmission, advertisement, and possession of child pornography.

5. Any and all records, documents, invoices, correspondence, notes and other materials that pertain to the ownership or use of computer equipment and other electronic equipment found in the residence and accounts with any Internet Service Provider, as well as any and all records relating to the ownership or use including sales receipts and billing information for Internet access, use or purchases made, including any associated registry information, logins, passwords, email addresses, screen names.

6. Credit/debit card or bank account information including but not limited to bills, statements, and payment records, which reflects payment for or purchase of computers or electronics, access to websites, software programs, organizations, groups, websites or other materials associated with child pornography.

7. Utility bills, rental agreements, and mortgage records which show the ownership, usage and/or possession of the searched premises.

8. Entry and exit photographs of the premises to be searched, as well as photographs of the specific places in which items are found and from which items are seized.